정보보안 관리 규정

제정 2011. 03.
개정 2014. 03.
개정 2015. 10.

제 1 장 총 칙

제1조(목적) 이 규정은 우송대학교(이하 '본교'라 한다)의 전산망 이용 시 내.외부의 무단 사용자에 의해 정보자산이 불법 유출.파괴 또는 변경되는 것으로부터 안전하게 보호하며, 모든 정보운영 환경과 응용프로그램을 보다 안전하게 운영함으로써 본교 전산망 사용자에게 원활한 서비스를 제공하고자 함을 그 목적으로 한다.

제2조(적용 대상과 범위) ① 이 규정의 적용 대상은 교내 전산자원을 사용하는 모든 정보시스템 및 그 이용자로 한다.

② 본교의 정보자산 보호와 정보운영환경 및 응용프로그램의 운영과 제공에 관하여는 따로 규정되는 경우를 제외하고는 이 규정에 따른다.

③ 정보보호에 대한 의무는 본교의 전산자원을 사용하는 구성원 모두에게 있으며 정보보안.관리규정을 준수할 의무가 있으며, 본 규정을 준수하지 않아 발생한 사고의 책임은 원칙적으로 사용자 본인에게 있다.

제3조(용어의 정의) ① "전산망"이라 함은 각종 정보시스템을 통신회선으로 연결하여 자료를 처리.보관하거나 전송하는 조직망을 말한다.

② "정보시스템"이란 정보의 수집, 가공, 저장, 검색, 송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.

③ "시스템관리자"라 함은 각 부서에 소속되어 시스템의 관리 권한을 가지고 전자적 민원처리 및 행정업무의 원활한 수행을 위하여 정보시스템을 운영·관리하는 사람을 말한다.

④ "데이터베이스관리자"라 함은 데이터베이스를 운영.관리하는 자를 말한다.

⑤ "전산자료"라 함은 전산장비에 의해 입력.보관되어 있는 정보자료를 말하며, 백업미디어 등 저장매체를 포함한다.

⑥ "정보보안" 또는 "정보보호"라 함은 정보통신 수단으로 수집.가공.저장.검색.송수신 되는 정보의 유출.위변조.훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적.물리적.기술적 수단을 강구하는 일체 행위를 말한다.

⑦ "시스템실"이라 함은 서버.PC 등 전산장비와 스위치.라우터 등 통신 및 전송 장비 등이 설치 운용되는 장소를 말한다.

⑧ "정보이용자(이하 "이용자"라 한다)"란 본교 전산망을 통하여 전자적 민원처리 또는 업무 담당자, 웹기반 서비스를 이용하는 민원인 및 시스템 관리자를 말한다.

⑨ "업무담당자"란 전자적 민원처리 또는 행정업무를 담당하는 사람을 말한다.

⑩ "민원인"이란 전자적 민원처리를 신청하는 주체로서, 개인 또는 사업자, 법인 등 단체 및 그 기관의 담당자 등을 말한다.

⑪ "본인확인"이란 정보통신망을 통하여 정보시스템 또는 행정정보를 이용하는 업무담당자, 민원인 또는 시스템 관리자가 가지고 있거나 알고 있는 정보를 이용하여 본인임을 확인하는 것을 말한다.

⑫ "접근권한"이란 정보시스템에 접속하여 정보자원을 활용할 수 있는 권한과 행정정보를 생성·변경·열람·삭제 등을 할 수 있는 권한을 말한다.
⑬ “개인정보”라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별 할 수 있는 정보(당해 정보만으로는 특정개인을 식별 할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.
⑭ “침해사고”라 함은 해킹, 컴퓨터바이러스, 악성코드, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.

제 2 장 위 원 회

제4조(구성) ① 체계적.효율적인 보안정책 수립. 심의 및 관리를 위하여 정보보안위원회를 둔다.
② 정보보호위원회는 정보화추진위원회와 통합하여 운영한다.
제5조(기능) 이 심사위원회는 제1조의 목적을 달성하기 위하여 다음 각 호의 사항을 심의.결정한다.
1. 정보보안정책 심의와 학내 정보보안의 총 관장
2. 정보보호 정책 및 총괄 계획 심의
3. 정보보안사고 처리의 책임을 심의.결정
4. 정보보안교육 및 정보보안준수 사항 감사
5. 기타 정보보안관련 제반업무의 총괄

제6조 (실무협의회 구성과 역할) ① 위원회 산하에 부서간 정보보안에 관한 업무협조를 위하여 ‘정보보안실무협의회’(이하 “협의회”라 한다)를 다음 각 호와 같이 둔다.(개정 2015.10.05.)
1. 협의회는 의장을 포함하여 15인내외의 위원으로 구성한다.
2. 위원은 정보보안 관련 주요부서 업무담당자나 권한 위임자를 당연직으로 하고, 그 밖에 전산전문위원이 추천한 관련분야 약간 명을 위원으로 포함 할 수 있다.(개정 2015.10.05.)
3. 의장은 전산전문위원이 겸임한다.(개정 2015.10.05.)
4. 의장을 포함한 각 위원의 임기는 보직재임기간 및 해당업무기간으로 한다.(개정 2015.10.05.)
5. 삭제(개정 2015.10.05.)

② 협의회는 각 부서의 담당자들이 업무를 수행하는데 있어 정보보안을 침해하는 일이 없도록 하기 위해 다음 각 호의 사항을 협의하여 결정된 사항을 정보보안심사위원회에 상정한다.(개정 2015.10.05.)
1. 각 부서 업무내역 중에 정보보안 시행세칙 작성(개정 2015.10.05.)
2. 시행세칙의 이행 및 관리감독
3. 기타 위 각 호에 부수되는 제반 사항

제 3 장 보 안

제7조(기본 수칙) ① 정보시스템 또는 행정정보 사용자는 개인별 사용자 계정 및 암호의 기밀을 유지해야 하며, 본래의 발급 목적으로만 사용하여야 한다.
② 교·직원 및 학생은 허가받은 정보시스템 또는 행정정보의 사용권한이 부여된 영역에 대하여 본래의 목적으로만 사용할 수 있다.
③ 정보시스템 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 아니

되며 위험을 초래할 수 있는 행위를 한 자가 발견된 경우에는 소속부서의 장 또는 정보보안담당부서에게 알려야 한다.

④ 정보시스템 또는 행정정보와 연관된 저작권.특허권 및 소프트웨어 라이센스의 사용 조건을 숙지하고 이를 준수하여야 한다. 또한 교내에서는 구매증서가 있는 합법적인 소프트웨어만 사용 할 수 있다.

⑤ 학내 전산망을 신설.변경 및 폐기하고자 하는 경우에는 정보보안담당부서의 사전승인을 얻어야 한다.

⑥ 외부 전산망에서 학내 전산망으로의 접근은 학교에서 승인한 정보시스템을 제외하고는 원칙적으로 허용하지 아니한다. 단, 필요시 적법한 절차에 따라 승인된 경우에 제한적으로 허용할 수 있다.

⑦ 모든 정보시스템 또는 행정정보는 보안등급에 따라 분류.관리한다.

⑧ 정보시스템 관리자는 주기적인 보안점검을 통해 학내 전산망 및 정보시스템의 안전성을 점검하고, 정보보안정책 및 규정의 준수 여부를 평가하며 학내 모든 사용자는 이에 적극 협조하여야 한다.

⑨ 업무와 관련해 습득한 정보자산을 본교의 허가 없이 외부에 누출해서는 아니 된다.

⑩ 또한 교내 각종 민감 정보 및 주요 연구자료의 교외이관 시 인터넷메일과 같은 사적 E-Mail을 사용할 수 없다.

⑪ 정보보안 사고를 예방하기 위한 목적으로 학교의 승인을 득한 정보보안시스템 및 정보보안 활동은 즉시 시행 할 수 있다.

제8조(보안등급 기준) ① 보안등급의 분류기준은 다음의 각 호에 따라 정한다.

1. 정보의 중요도
2. 정보시스템 또는 행정정보의 절취 및 불법변경 시 손실 가치
3. 정보시스템 또는 행정정보의 파괴 시 복구비용
4. 행정정보의 사용권자

② 정보시스템 또는 행정정보의 보안등급 및 사용자 인가는 전항의 기준에 따라 행정정보를 보유한 부서의 장이 별도로 정한다.

제9조(보안 점검) ① 정보보안담당부서는 교내 주요서버 및 각 연구실의 서버에 대해 필요시 수시 점검을 실시 할 수 있으며 다음 각 호의 단계를 따른다.

1. 보안점검 대상 및 분야를 해당 부서에 통보한다.
2. 해당 부서에서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비 한다.
3. 보안점검을 실시한 후 그 결과를 위원회 위원장에게 보고한 후 해당 부서에 통보한다.
4. 해당 부서에서는 지적사항을 즉각 시정하고 그 결과를 위원회 위원장에게 보고 한다
5. 정보보안담당부서는 필요시 각 부서의 보안점검 지적사항에 대한 시정 여부를 확인할 수 있다.

② 홈페이지 침해사고 및 개인정보노출사고 등을 예방 및 대처하기 위해 다음 각 호에 따라 정보보안담당부서는 보안점검을 실시 또는 요구할 수 있다.

1. 보안점검 대상은 본교 모든 홈페이지로 한다.
2. 보안점검은 홈페이지를 구축 할 때와 점검사유가 발생할 때 실시한다.
3. 보안점검은 원칙적으로 정보보안담당부서에서 시행하나, 사전 협의된 경우 구축·관리 주최에서 자체적으로 보안점검을 진행하고, 그 점검결과를 정보보안 담당부서에 통보할 수 있다.
4. 위 ①항에 따라 보안점검을 실시한다.

제10조(보안사고의 처리) 보안사고가 발생할 경우 정보보안담당부서는 다음 각 호의 단계에 따라 적절한 조치를 취하여야 한다.

1. 침입자의 침입예방을 위하여 침입 가능성이 있는 부분을 수시로 점검하여 불법침입자의 침입을 사전에 예방한다.
2. 시스템관리자는 자신의 시스템에 비정상적인 활동이나 징후가 보이면 무단 침입자의 유무를 즉각

점검해야 한다.

3. 침입자가 현재 시스템에 침투해 해킹을 하고 있을 경우 필요한 조치를 즉각 취하고 보고하여야 한다.

4. 침입자를 몰아냈거나 로그파일의 분석을 통해 침입한 흔적이 발견된 경우 즉시 보고 하고, 보안진단 도구나 체크리스트를 이용하여 정보자료의 이상 유무를 점검하여야 한다.

제11조(보안 교육) ① 학내 의사결정자, 데이터베이스관리자, 업무담당자 및 시스템 관리자를 대상으로 정보보안교육을 실시한다.

② 보안교육은 주제별, 대상별 필요에 따라 수시/정기교육을 실시한다.

제12조(정보보안담당관) ① 본교의 효율적인 정보보안 업무를 수행하기 위하여 '정보보안담당관'을 둔다.

② 정보보안담당관은 전산정보담당관으로 한다. (개정 2014.03.01.)

제13조(정보보안 기본활동) 정보보안담당관은 정보보안을 위하여 다음 각 호의 기본활동을 수행하여야 한다.

1. 정보보안 정책 및 기본계획 수립.시행
2. 정보보안 관련 규정.지침 등 제.개정
3. 정보보안담당관 및 보안심사위원회 운영
4. 정보보안 업무 지도.감독
5. 정보보안 감사 및 심사분석
6. 정보보안 관리실태 평가
7. 사이버공격 초동조치 및 대응
8. 사이버위협정보 수집 . 분석 및 보안관제
9. 정보보안 예산 및 전문인력 확보
10. 정보보안 사고조사 결과 처리
11. 정보보안 교육 및 정보협력
12. 주요 정보통신기반시설 보호활동
13. 보안시스템 및 암호키의 운용.보안관리
14. 정보통신망 보안대책의 수립.시행
15. 기타 정보보안 관련 사항

제 4 장 정보시스템 관리

제14조(사용자 정의) 정보시스템 또는 행정정보를 사용할 수 있는 자는 다음 각 호와 같다.

1. 본교 교원, 직원, 재학생 및 졸업생
2. 연구소 및 부속기관의 장이 사용을 인정한 자

제15조(적절성 확보) 정보시스템 또는 행정정보 이용자는 정보시스템 사용에 있어 적절성을 유지하여야 한다. 다만, 다음 각 호에 해당하는 경우에는 부적절한 사용으로 간주하여 제재 조치를 취할 수 있다.

1. 타 사용자의 계정 및 암호를 허가 없이 사용한 경우

2. 타 사용자의 정당한 사용을 방해한 경우
3. 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 행위
4. 일반사용자가 관리계정 암호 또는 타 사용자의 암호를 획득하고자 해킹하는 행위
5. 내부의 중요 전산정보를 불법으로 외부에 유출한 경우
6. 외부의 불법사용자에게 계정 및 암호를 제공한 경우
7. 사용자 계정 및 암호를 상호 공유하는 행위
8. 시스템관리자가 특별한 사유 없이 관리계정 암호를 일반사용자와 공유한 경우
9. 허가된 보안등급 이상의 자료를 무단유출 하거나 읽고 쓰는 행위
10. 인터넷을 통해 자살 또는 음란 사이트 등 반사회적인 유해사이트에 접속.개설.열람하는 경우
11. 보안점검의 지적사항에 대해 즉각적인 시정을 취하지 않는 경우
12. 정보시스템을 이용한 개인정보 침해사고(불법유출, 훼손, 갈취, 불법열람 등)가 발생한 경우

제15조2(대학정보시스템 권한관리 및 비밀번호관리) 대학정보정보시스템을 사용하고자 하는 전체 교직원 및 재적 학생은 다음의 정책을 준수하여야 한다.(신설2015.10.05.)

①재직중인 교직원으로서 대학정보시스템의 업무 권한을 부여 받고자하는 자는 부서장의 승인을 받아 필요한 업무권한을 신청하여 업무에 활용할 수 있다.

②대학정보시스템의 권한을 부여 받은 자는 다음 각 호의 비밀번호 정책을 준수하여야 한다.

1. 사용자 계정과 동일하지 않을 것
2. 개인신상 및 부서 명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어는 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 말 것
5. 한번 사용된 비밀번호는 재사용하지 말 것
6. 비밀번호는 문자, 숫자, 특수문자를 혼합하여 9자리이상으로 설정할 것
7. 설정된 비밀번호는 절대 타인과 공유하지 말 것

제16조 (사용자 제재) ① 제14조 각호에 규정된 사항에 해당할 경우에는 사용자의 계정을 회수.삭제하여 정보시스템 또는 행정정보의 사용을 제한 또는 금지하며, 그에 따른 구체적 제재사항은 위원회에서 심의. 결정한다.

② 정보시스템 또는 행정정보의 불법사용으로 학교에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각 호의 제재조치를 취할 수 있다.

1. '정보통신망 이용촉진 및 정보보호 등에 관한법률, 부정경쟁방지 및 영업비밀 보호에 관한법률' 등 관련 법령에 의한 법적조치
2. 학칙 및 관련 규정에 따른 징계 조치
3. 공공기관 개인정보보호에 관한 법률에 의한 조치
4. 정보시스템의 손해발생에 대한 손해배상 청구

제 5 장 네트워크 관리

제17조(전산망 관리) ① 네트워크관리는 일관성과 기밀성을 위해 통합관리를 원칙으로 한다.

② 운영부서의 관리자는 네트워크 신규설치 및 변경 시 정보보안담당부서에 변경정보를 통보해야 한다.
③ 네트워크 IP ADDRESS는 사용자가 임의로 변경할 수 없다.
④ 라우터 패스워드는 제21조에 규정된 계정관리에 따른다.
⑤ 인터넷을 이용한 모든 외부로부터의 접근은 원칙적으로 금지한다. 단, 다음과 같은 적절한 사유와 승인절차를 거친 경우에 한해 허용 할 수도 있다.
1. 연구를 목적으로 원격접속이 필요한 경우
2. 정보시스템과 관련한 원격 업무지원이 필요한 경우
⑥ 정보시스템에 대한 원격접속을 허용할 경우 다음을 준수하여야 한다.
1. 원격접속 작업자는 보안서약서를 제출해야 한다.
2. 원격접속 작업자에게는 작업에 필요한 최소 권한만을 부여한다.
3. 원격접속 작업자는 해당 시스템관리자 또는 업무담당자의 관리·감독 하에서만 접근하게 한다.
4. 원격접속은 업무시간 범위에서만 허용한다.
5. DB서버와 같은 보안등급 최상위 정보시스템은 원격접속 대상에서 제외한다.
⑦ 일정횟수 접속실패 시 접속을 차단하고 관련 정보를 로그에 기록한다.
⑧ 보안상 취약한 무선 통신망의 신설 또는 증설은 억제한다.

제18조(네트워크의 보호) ① 정보보안담당부서는 본교에 유해하거나 불필요하다고 판단되는 웹사이트 접속을 통제할 수 있다.
② 원격 사용자의 공중망 네트워크를 통한 접속은 인증 시스템 또는 방화벽에 의해 통제할 수 있다.
③ 신뢰할 수 없는 정보시스템 및 서버로의 접속을 보호하기 위해 네트워크 정책을 설정하여 통제 할 수 있다.
④ 네트워크 보안 담당자는 의심스러운 활동에 대해서는 방화벽, 침입탐지시스템(IDS) 및 기타 보안 시스템의 로그를 분석하여 해당내용을 확인하여야 하며 필요시 부서장에게 보고해야 한다.
⑤ 교내 네트워크 사용 시 적법한 사용자임을 인증 받아야 하며, 사용하는 정보시스템 역시 적정 무결성 수준 및 보안수준을 점검하여 본교 정보보안 기대수준에 미달 시 네트워크 사용을 제한 할 수 있다.
⑥ 무선통신 네트워크를 구축 시 무선중계기(AP)의 전파범위 조정, 사용자 인증, 패킷 암호화 등 보안대책을 적용하여 구축 한다.

제 6 장 서버 관리

제19조(운영 및 관리) ① 신규 임용된 교원과 직원의 계정 등록요구 시 시스템 관리자에게 사용목적.사용기간 및 연락처 등을 제출하도록 한다.
② 휴직자의 계정은 휴직기간동안 일부 서비스로 제한 할 수 있다.
③ 퇴직자는 사직원 제출 시 사용자 계정을 일부 서비스로 제한 할 수 있다.
④ 시스템 관리자는 최소 월 단위로 사용자의 패스워드를 체크해 취약한 패스워드가 발견될 경우 당사자에게 통보하여 변경을 요구할 수 있다.
⑤ 취약한 패스워드를 사용한 계정에 대해서는 경고를 하되, 2회 이상의 경고를 받고도 변경하지 않을 경우에는 1개월 동안 계정을 폐쇄할 수 있다.
⑥ 시스템 개발 및 운영부서의 장은 응용프로그램 개발계획 단계에서 보안정책에 근거한 응용프로그램 개발을 지시하고, 이를 위반할 경우에는 개발을 중지시킬 수 있다.
⑦ 슈퍼유저의 권한은 정보보안업무 담당자/시스템 관리자로 제한한다.

⑧ 장애복구나 점검을 위해 루트 권한을 위임할 경우에는 시스템 관리자 입회하에 작업을 실시하고, 작업종료 후 루트계정과 패스워드를 변경한다.
⑨ 백업지침은 별도로 정하며, 반드시 지침에 따라 주기적인 백업을 실시한다.
⑩ 각 부서는 백업 미디어별로 적절한 사용연수를 정하여 노후 된 백업미디어에 대해서는 사용하지 아니 한다.

제20조(보안관리) ① 전체 시스템에 대한 보안 관리와 전반적인 방향설정 및 주기적인 보안점검은 정보보안담당부서에서 실시한다.
② 개별 서버에 대한 보안 관리는 각 서버의 관리자가 담당한다.

제21조(계정관리) ① 사용자 계정 분류는 그 사용목적에 따라 분류하고 그 기준은 따로 정한다.
② 사용자별 또는 그룹별로 접근권한을 부여한다.
③ 외부 사용자의 계정은 유효기간을 설정한다.
④ 특별한 사유 없이 1학기 이상 사용하지 않는 계정은 학기 시작 일주일 이내에 말소한다.
⑤ 암호가 없는 계정은 사용을 금지한다.
⑥ 일정회수 접속 실패 시 사용을 금지한다.
⑦ 슈퍼유저는 Console 및 특정 단말기에서만 접속을 허용한다.
⑧ 사용자 계정절차의 등록.변경 및 폐기는 다음을 따른다.
1. 사용자 계정은 사용자 등록이나 변경 또는 폐기 신청서를 작성한 후에 시스템 관리자에게 통보하되, 외부사용자는 반드시 사용기간 및 목적 등의 사유를 명확히 해야 한다.
2. 시스템관리자는 내용을 검토한 후에 사용자 계정을 등록이나 변경 또는 폐기하고 사용자에게 그 사실을 통보한다.
3. 사용자 계정을 등록하거나 변경 또는 폐기할 경우에 일반적인 사항은 월 단위로 부서장에게 사후 보고한다. 다만, 특별한 상황이 발생할 경우에 한하여 부서장의 허가를 받은 후에 작업을 실시한다.

제 7 장 전산자료 및 데이터베이스 관리

제22조(자료의 관리) ① 데이터베이스 로그인 계정 관리기준은 DBMS 관리자(DBA).응용프로그램 개발자 및 사용자에 따라 권한을 차등 부여하고, 패스워드는 암호화된 형태로 존재하도록 한다.
② 데이터베이스의 무결성 유지를 위해 데이터베이스의 수정은 적법한 인가자에 의해서만 이루어져야 하며, 물리적인 재해로부터의 보호를 위해 주기적으로 백업하여야 한다.
③ 데이터베이스에 대한 모든 접근은 감사기록을 유지하되, 일반사용자의 감사기록에 대한 접근은 제한해야 한다.
④ 데이터베이스 관리자(DBA)는 누가 어떤 필드, 레코드 수준에서 접근할 수 있는가를 정의해야 한다.
⑤ DBMS는 시스템과는 별도의 사용자 인증기능을 수행해야 한다.
⑥ 데이터베이스의 데이터는 응용프로그램을 통해서만 접근한다.
⑦ 별도지침에 의해 중요자료로 분류된 자료 및 데이터베이스는 데이터의 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제23조(자료의 보관) ① 별도지침에 의해 중요자료로 분류된 자료는 별도의 보호된 장소에 보관하고, 재해 및 비상시에 대비해 소산계획을 수립하여 운영한다.
② 별도지침에 의해 중요자료로 분류된 자료의 이용 및 변경은 부서장의 허가와 관리책임자의 입회하에 이용 및 변경할 수 있다.

제24조(자료의 파기) ① 별도지침에 의해 중요자료로 분류된 자료의 파기는 자료보관책임자의 입회하에 담당자가 파기를 실시하고, 자료관리 대장의 파기 확인란에 입회자는 파기 확인을 한다.
② 자기테이프 등의 자기매체 자료의 파기는 컴퓨터를 이용하여 내용을 완전히 삭제하고, 자료접근이 불가능해 내용을 지울 수 없는 자기매체의 자료는 소각 또는 용해 등의 방법으로 파기한다.
③ 출력된 자료는 사용 목적이 완료되어 폐기 시에는 반드시 문서파쇄기를 이용하여야 한다.

제 8 장 응용프로그램 관리

제25조(응용프로그램 개발) ① 모든 응용프로그램은 접근하는 데이터의 정보등급에 따라 해당 응용프로그램의 보안등급을 설정한다.
② 응용프로그램의 계획서 및 설계서는 보안관리 규정에 근거하여 보안대책이 마련되어야 하며, 프로그램 개발 시에 이를 반영해야 한다.
③ 별도지침에 의해 중요자료로 분류된 응용프로그램은 정보보안을 위해 사용자계정 및 암호를 설정해야 한다.
④ 응용프로그램에서 사용하는 사용자계정.암호 및 기타 전산망 접근과 관계된 중요정보는 소스코드로부터 분리하여 1차 인식이 불가한 암호화된 형태로 존재해야 한다.
⑤ 별도지침에 의해 중요자료로 분류된 응용프로그램은 개발 시 시스템 사용에 대한 로그정보를 관리함을 원칙으로 한다.
제26조 (응용프로그램 운영) ① 응용프로그램 운영자는 응용프로그램 사용자 계정에 대한 암호 변경을 최소 6개월에 1회 이상 실시해야 한다.
② 응용프로그램 운영자는 시스템 사용에 대한 로그 정보를 주기적으로 분석하여 자료의 불법접근 및 변조에 대한 위험성을 사전에 방지해야 한다.
③ 응용프로그램의 버전관리는 소스프로그램과 실행프로그램의 버전이 일관성을 유지하도록 한다.
④ 개발된 응용프로그램의 복제는 시스템관리자의 사전양해와 입회하에 실시해야 한다.
⑤ 응용프로그램의 추가.삭제 또는 변경은 부서장의 허가를 받은 후에 시스템 관리자에 의해 실시되어야 한다.
⑥ 운영 중인 시스템에는 응용프로그램의 소스프로그램을 설치하지 않는 것을 원칙으로 한다.
⑦ 별도지침에 의해 중요자료로 분류된 응용프로그램은 가동 전 정보보안담당부서의 보안검증을 받아야 한다.

제 9 장 PC 관리

제27조(PC의 관리) ① PC 기동 시 CMOS에서 제공하는 패스워드를 설정한다.
②PC에는 로그인 비밀번호 및 비밀번호가 설정된 화면보호기를 작동시켜야 하며 화면보호기의 설정시간은 10분 이내로 한다.(개정 2015.10.05.)
③ 장시간 자리를 비울 때는 전원을 끈다.
④ 자신의 업무에 사용하는 응용 프로그램은 시스템 보안관리자의 허락 없이 무단으로 타인에게 복사해 주어서는 아니 된다.
⑤ 휴대용 저장매체를 통한 자료의 전송을 금지한다. 다만, 업무상 부득이한 경우 등록된 휴대용 저장매

체를 활용하여야하고, 그 사용 내역을 대장에 작성하여 부서장의 통제를 받아야 한다.(개정 2015.10.05.)
⑥ 업무상 중요한 정보는 PC내에 보관하지 아니 하며, 별도의 등록된 저장매체 담아 물리적인 보안이 철저한 위치에 보관한다.(개정 2015.10.05.)
⑦단말기 사용자는 PC、노트북、PDA 등 단말기(이하 PC 등) 사용과 관련한 일체의 보안관리 책임을 가진다. 또한, 운용중인 운영체제(OS) 및 응용프로그램(한컴 오피스, MS Office, Acrobat 등)의 최신 보안패치 유지하여야 한다. (신설 2015.10.05.)
⑧업무상 불필요한 응용프로그램의 설치를 금지하고, PC의 시스템 자원(폴더, 파일 등)에 대한 공유는 모두 제거되어야 한다. 다만, 필요에 의해 공유할 경우에는 패스워드 설정, 보안인증, 암호화 등의 보안대책을 수행하여야 한다. (신설 2015.10.05.)
⑨사용자는 PC 등 단말기를 교체、반납、폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 관리책임자와 협의하여 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치 하여야 한다. (신설 2015.10.05.)
⑩ 개인소유의 PC(노트북 PC 등)는 부서 내부로 반입 또는 반출하여 사용하여서는 아니 된다. 다만, 부득이한 경우에는 정보보안담당관의 승인을 받아 보안조치 한 후 반입 또는 반출 할 수 있다. (신설 2015.10.05.)

제28조(바이러스 예방 및 조치) ① 정보보안담당부서는 컴퓨터 바이러스, 웜발생으로 심각한 피해가 우려되는 경우 게시판이나 메일 등을 통해 경고 메시지 게시 등의 조치를 취한다.
② 교내 전산망을 통해 전산자원을 사용하는 모든 PC는 웜, 바이러스 감염을 예방하기 위해 아래와 같이 조치해야하며, 정보보안담당부서는 필요하다고 판단될 경우 이를 강제할 수 있다.
1. 본교 정보보안 담당부서에서 인증한 바이러스 백신프로그램을 설치하여야 한다.
2. 설치된 바이러스 백신 프로그램을 항상 최신 버전으로 유지해야 한다.
3. 정기적인 바이러스 검색을 통해 예방과 치료에 노력해야 한다.
③ 바이러스에 의한 데이터 손상에 대비해 정기적으로 데이터 백업을 실시한다.
④ 정보보안담당부서는 알려진 바이러스의 경우에는 해당 바이러스를 치료할 수 있는 진단 프로그램을 구비한다.
⑤ 무단, 불법 복사된 프로그램을 설치한 정보시스템은 교내 전산망 접속을 제한한다.
⑥ 바이러스의 감염이 확인될 경우 즉각 네트워크 접속을 단절시킨 후 바이러스백신 프로그램으로 바이러스를 치료한다.
⑦ 외부에서 온 디스켓, 인터넷에서 다운로드 받은 파일, 외부로부터 전송된 메일의 첨부파일 등은 실행 또는 열기 전에 반드시 바이러스 검사를 해야만 한다.

제 10 장 시스템실 운영.관리

제29조(시스템실 시설기준) ① 출입구에 입실자를 식별 및 통제 가능한 출입보안장치를 설치한다.
② 자동화재경보 설비를 설치하고, 할로겐 가스 등 소화 시 장비에 피해를 주지 않는 자동소화 설비를 설치한다.
③ 정전에 대비하여 별도의 전원공급 시설을 둔다.
④ 온、습도를 적절히 유지할 수 있는 항온항습기를 설치한다.

제30조(시스템실 운영 및 관리) ① 시스템실의 운영을 담당하고 있는 부서장은 시스템실 사용 및 운영에 관한 절차 및 방법을 규정하고, 담당자들이 이를 숙지하도록 한다.
② 시스템실의 운영자는 운영일지 및 장애일지를 작성해야 한다.
③ 시스템 운영자는 주기적으로 로그화일을 분석해야 하며, 시스템에 이상이 발견되었을 경우에는 보안사고처리 지침에 따라 즉시 조치를 취하고 이를 정보보안담당부서장 및 해당 부서장에게 보고해야 한다.
④ 시스템실에는 출입자 명부를 비치하고 비인가자의 출입을 통제해야 한다.
⑤ 시스템실.자료보관실 및 통신실은 관리책임자를 지정하고 자료 또는 장비별로 취급자를 지정 운영해야 한다.

제 11장 개인정보 보호

제31조 (개인정보 관리) ① 개인정보 관리는 수집, 이용, 제공, 보관 및 파기 등으로 구분되며 관련 법률을 준용하여 취급한다.
② 본교에서 업무상 개인정보를 취급하는 사용자는 개인정보취급자라하며 개인정보 보호를 위해 개인정보 취급 시 본 규정과 관련 법률을 준수하여야 한다.
제32조 (개인정보 보호) ① 개인정보 수집은 다음과 같이 한다.
1. 개인정보는 법적근거와 정보주체의 동의획득을 통해서만 수집될 수 있다.
2. 개인정보는 소관업무에 필요한 최소한의 정보만 수집되어야 하고 민감한 개인정보는 수집하지 않는다.
3. 개인정보 수집 시 정보주체에게 법적근거, 수집목적, 이용범위, 정보주체의 권리 및 보유기간을 고지한다.

② 개인정보의 이용 및 제공은 다음과 같이 한다.
1. 개인정보는 수집 목적으로만 이용한다.
2. 개인정보의 이용 요청과 제공은 문서로 처리한다.
3. 개인정보는 법률이 정하는 경우와 본인 동의가 있는 경우에만 제3자에게 제공한다.
4. 개인정보의 취급위탁 시 위탁사실을 공개하고 본인 동의를 득한다.

③ 개인정보의 보유 및 파기는 다음과 같이 한다.
1. 개인정보가 분실, 도난, 누출, 변조 및 훼손되지 않도록 안정성 확보에 필요한 기술적·관리적 보호조치를 한다.
2. 개인정보가 수집목적을 다해 보유가 불필요하게 된 경우, 보유기간이 만기된 경우에는 지체 없이 파기한다.

제 12 장 기 타

제33조(시행규칙) 이 규정의 운용에 필요한 세부사항은 시행규칙으로 따로 정할 수 있다.
제34조(준용) 기타 이 규정에 명시되지 아니한 사항은 본교의 관계 규정에 준한다.

부 칙

제1조 (시행일) 이 규정은 2011년 3월 2일부터 시행한다.

부 칙

제1조 (시행일) 이 규정은 2014년 3월 1일부터 시행한다.

부 칙

제1조 (시행일) 이 규정은 2015년 10월 1일부터 시행한다.